3.0 TECHNICAL

3.1 Facilities

Since patient care operations are reliant on building systems, it is essential that these systems not experience any failures or degradation in operations due to Year 2000-related problems. The Veterans Health Administration (VHA) developed the "Health Care Facility Y2K Utility Systems Guidebook" to assist VA health care facilities with addressing and preparing for potential Year 2000-related utility systems problems. The Guidebook was published in January 1999. Subject matter experts from the field worked in collaboration with the staffs of the Chief Network Officer and the Chief Information Officer to produce this document. Staff should pay particular attention to the utility systems matrices and contingency plan testing portions of the Guidebook.

A second and significantly improved, updated edition of the "Health Care Facility Year 2000 Utilities Guidebook" will be shipped to the field in the near future. This update edition has a number of improvements that will assist in Year 2000 readiness activities at all VA and non-VA health care facilities. In addition to the number of improvements added, this Year 2000 Utilities Guidebook was edited to remove specific VA reference; so, it will be applicable to private health care facilities. Until this publication is distributed, continue using the current edition of the existing Utilities Guidebook. Extra copies can be obtained from the VA National Engineering Service Center by calling 314.425.4950.

3.2 Medical Devices

The Year 2000 problem has been recognized as much as a management challenge as a technical problem. Assessing, renovating, validating and preparing contingency plans for medical equipment for the Year 2000 is no different. The “Year 2000 Medical Device Assessment Guidebook” in Appendix E describes practical approaches to managing Year 2000 compliance issues for medical equipment used in the health care facility. It is organized into four major chapters:

- **Awareness** - describes and communicates the scope of the Year 2000 compliance issues for medical devices to facility staff.
- **Assessment** - combines available compliance information with local medical equipment inventory and tracks required action.
- **Renovation/Implementation** - describes action(s) necessary to correct identified Year 2000 problems for medical devices.
- **Validation** - describes action(s) necessary to assure implementation is effective, including contingency planning.

When developing contingency plans for medical devices, staff should pay particular attention to the chapter on validation and Appendix D, which is a guideline for a medical equipment contingency plan.

The guidebook is an improved version of the previous edition titled "Veterans Health Administration, Year 2000 Compliance for Medical Equipment" published by the National Cost Containment Center in September 1998. In addition to a number of improvements that were made, this version of the guidebook does not contain specific VA references and acronyms; so, it is applicable to private health care facilities. Over 2000 copies of this "generic" version of the

Medical Equipment Guidebook have already been distributed by VHA as a public service outreach effort with assistance by the American Hospital Association. VA health care facilities are encouraged to share this generic version of the Year 2000 Medical Equipment Guidebook with private health care facilities.

3.3 Telecommunications

3.3.1 Background

A potential for failure exists for telecommunications and data communications - such as Local Area Network (LAN) and Wide Area Network (WAN) - components before, during and after January 1, 2000. This is due to the standard practice of using two digits to represent the year in computer databases, software applications and hardware chips.

Difficulties may arise when devices that process dates attempt to perform calculations on the year “00” and erroneously process it as 1900 rather than 2000. This could potentially cause systems to fail altogether, or continue to function while corrupting data. If corrupted data goes unrecognized, the problem could affect telecommunication interfaces.

Other problems may involve systems’ logic that will not recognize the Year 2000 as a leap year, has triggers that are executed based on specific values in the date field(s), or have overflow and/or rollover problems.

Traditional contingency plans and recovery systems do not address the issue of them being affected by the same problem(s) as the primary system.

This section provides a road map of actions that will streamline decision-making and outlines the Telecommunications Contingency Planning template for VHA’s voice and data communications systems. When exposure to year 2000 problems are at a peak, effective planning will greatly reduce the number and magnitude of decisions that must be made.

3.3.2 Pre-Year 2000 Preparations

The assumption is that both professional experience and due diligence have been used in assessing, renovating and testing all telecommunication systems and equipment. A contingency plan and system recovery procedure should still be developed and tested to address the possibility that failure(s) may occur before, during or after Year 2000 due to the following:

- All non-compliant systems and equipment may not have been identified.
- All Year 2000 corrections may not be developed/installed on time.
- New compliant replacement systems may not be installed due to lack of time and/or funding.
- External interfaces may infect systems with bad date-related data.

The telecommunications network at most VAHCFs consists of a Voice System, LAN and a connection to the VHA WAN. An assessment of the risks in each of these three major areas is necessary, in order to develop adequate contingency plans for telecommunications. When performing the assessments, include: the potential Year 2000 impact on end-users, critical care providers, equipment manufacturers and vendors. All of the Year 2000 compliant components must function as a whole in order for the telecommunication system to function properly.

a. *Monitor and Assess Year 2000 Compliance of Voice Systems*

The VAHCF voice system may include: a Private Branch Exchange (PBX) switch, Voice Mail, access to local and long distance service, Telephone Management System, Call Detail Recording (CDR), Automatic Call Distribution(ACD) system, Attendant Consoles and station equipment, such as telephones.

If the PBX switch fails, it is likely that the VAHCF will not be able to place or receive telephone calls. It is therefore very important to monitor the compliance status of the PBX system that is being used at the VAHCF. Access to local telephone service is also imperative for calls to be made, so the compliance status of the local Telephone Company should also be monitored closely. The other features are peripheral to the operation of the voice system and are not critical to placing and receiving telephone calls.

By early to mid-September 1999 the VAHCF should evaluate the progress of the equipment manufacturers and local telephone company towards compliance. If it is determined that the equipment will not be compliant in time, they should begin acquiring alternate resources such as cellular phones and two-way radios.

b. *Monitor and Assess Local Area Network Compliance*

The Local Area Network (LAN) may include workstations, servers (BootP, DNS, and E-mail) hubs, routers, firewall, intelligent bridges, modems and network management platforms.

If the LAN fails, any intelligent workstations (Personal Computers) can be used in stand-alone mode. Network printers can be disconnected from the network and connected to PCs. Patient information would not be readily accessible, so manual procedures would have to be implemented until the LAN is restored. Prior to transition of the century, it is necessary to closely monitor the compliance status of LAN components to ensure continued availability of the LAN and associated resources.

By early to mid-September 1999 the VAHCF should evaluate the progress of the equipment manufacturers towards compliance. If it is determined that the equipment will not be compliant in time, they should begin considering activation of manual procedures

c. *Monitor Wide Area Network Compliance*

The Wide Area Network (WAN) may include: servers, gateways, firewalls, switches and network management platforms.

If the WAN fails, as long as no patient data needs to be transferred, this is not a mission critical function. However a failure of the WAN would mean no information can be transferred to the VISN office or another VAHCF. If available, such information can be transferred by fax, telephone or courier.

The VA Wide Area Network Office is closely monitoring the compliance status of the WAN. Prior to transition of the century, each VAHCF must obtain the necessary assurance from the WAN Office regarding the availability of wide-area service.

3.3.3 Execution Phase

a. *Check Voice System Availability*

Shortly after midnight on January 1st, 2000, pick up the telephone and check for dial tone. Make telephone calls to different services (check the local, long distance and FTS telephone services).

Report the status of the Voice (PBX) Systems to the VAHCF Command Center.

b*. Check Local Area Network Availability*

Shortly after midnight on January 1st, 2000, make sure servers, hubs and other LAN equipment are functioning correctly. Send a test e-mail message from one workstation to another on the same server. Then send an e-mail message from one workstation to another workstation on a different server.

Report the status of the LAN Systems to the VAHCF Command Center.

c*. Check Wide Area Network Availability*

Shortly after midnight on January 1st, 2000, make sure WAN servers, gateways, firewalls, gateways and switches are functioning correctly. Send a test e-mail message to another VAHCF. Then send an e-mail message to the VISN office.

Report the status of the WAN to the VAHCF Command Center.

d*. Role of the Business Resumption Team*

The Business Resumption Team will be executing the Contingency Plans, reporting the status of telecommunications systems, and referring management decisions to the Command Center. The Command Center will be responsible for updating the VISN on the status of critical systems. Section 2.1.4.4. Internal Operations outlines the specific duties and membership of the Business Resumption Team.

3.3.4 Post-Execution Phase

a. *Evaluate Voice System Failures & Restoration Procedures*

See Telecommunications’ Failures and Restoration Checklist (Figure 2, page 31)

Figure 2

Telecommunications’ Failures and Restoration Checklist

Voice Component	**Failed (yes/no)**	**Type of and Time to Restoration (hrs/days/weeks/months)**
Telephone switch		
Voice mail		
Access to local phone service		
Access to long distance phone service		
System management		
Call detail recording		
Automatic call distribution		
Add, move and change services		
Attendant consoles		
Station Equipment (phones)		
LAN Component	**Failed (yes/no)**	**Type of and Time to Restoration (hrs/days/weeks/months)**
Boot P servers		
DNS server		
E-mail server		
Hubs		
Routers		
LAN management platforms		
Network time protocols		
Wireless LAN		
WAN Component	**Failed (yes/no)**	**Type of and Time to Restoration (hrs/days/weeks/months)**
Servers		
Firewall		
Router		
Gateway		

b. *Evaluate Local Area Network Failures & Restoration Procedures*

See Telecommunications’ Failures and Restoration Checklist (Figure 2, above)

c. *Evaluate Wide Area Network Failures & Restoration Procedures*

See Telecommunications’ Failures and Restoration Checklist (Figure 2, above)

d. *Evaluation of Lessons Learned*

Compile a report by evaluating the Voice, LAN and WAN failures, and the lessons learned as a result of these failures. This report should also include information concerning the restoration procedures, lengths and costs.

e. *Update Contingency Plan*

Changes and updates to the contingency plan should be based on lessons learned during the execution phase.

3.3.5 Summary

This Year 2000 telecommunications contingency plan should establish, organize and document the following:

- Risk assessments
- Staff responsibilities
- Policies and procedures
- Agreements and understandings between all internal and external entities

All personnel should be trained, and the plan and its checklists should be tested and updated regularly to reflect "lessons learned" and changes in telecommunications. For further information on FTS, refer to GSA's FTS Telecommunication Contingency Plan on the GSA WebSite. Be aware that the need exists to modify telecommunications' contingency plans as contracts or vendors change the compliance status of equipment, and/or testing identifies other changes.

3.4 Automated Information Systems

It is essential that VA health care facilities have contingency plans in place so that Automated Information Systems that support patient care are not interrupted due to Year 2000-related problems. VA and OMB guidelines mandate that all VA health care facilities should have contingency plans for their Automated Information Systems (AIS). Since the Year 2000 problem poses a number of new and unique threats to the continuity of information systems, current contingency plans should be reviewed for appropriateness and updated as needed. Contingency planning should include the identification of potential problems, their impact on mission-critical systems, and policies and procedures to minimize any potential disruption in operations. A list of potential AIS system failures that could occur as the result of Year 2000 date-related problems is provided in supplement 1, page 46.

Contingency plans and system recovery procedures should be developed and tested to address the possibility that failure(s) may still occur before, during or after transition of the century due to:

- Not all non-compliant systems and equipment were identified.
- Renovation of non-compliant AIS equipment or systems was not implemented due to lack of time or funding.
- A system's functionality was lost due to the reliance on a non-compliant external interface.

3.4.1 Pre-Year 2000 Preparations

The Chief, IRM or Chief Information Officer should be responsible for coordinating the development of a facilitywide Year 2000 contingency plan for Automated Information Systems. The Chief IRM should oversee an AIS Year 2000 Contingency Planning Team, composed of technical experts who will develop and implement Year 2000 contingency plans for AIS systems. Membership of the AIS Team should include, the ***VISTA*** Systems Manager, Information Security Officer, supervisor of telecommunications, and network manager. The AIS Team should coordinate their efforts with the health care facility's Business Continuity Planning Workgroup (BCPW) so that AIS contingency plans are integrated into the over-all health care facility's Year 2000 Contingency Plan. The membership and responsibilities of the BCPW are detailed in section 2.1.3 of the Year 2000 Contingency Planning Guidebook.

The AIS Team should:

- Review all AIS hardware and software for Year 2000 compliance and correct any deficiencies.
- Work with the Functional Unit Managers to determine the criticality of AIS systems. This can be accomplished by reviewing the AIS portion of the functional unit templates.
- Assess the probability (risk) of a Year 2000-related failure and the need for back-up plans/systems for each critical AIS system.
- Prepare a priority list of systems, servers and desktop hardware and identify those that are "mission critical." Priorities will be based on equipment that has been identified as "mission critical" (i.e., patient care areas, laboratory and central servers).
- Identify back-up equipment and software for critical systems to be held in reserve as replacements if failures occur. This extends to vendors and back-up media needed to back up systems.
- Ensure that "mission-critical" systems such as servers, hubs, telephone closets, telephone switches, and key clinical workstations are on emergency power.
- Prepare for adequate coverage and appropriate IRM staff to cover during the Execution Phase. Prepare a "triage" plan for IRM to respond to various scenarios.
- Prepare a phone list including number of pagers and portable phones of key staff for use by Business Resumption Team and the Command Center. Identify necessary vendor support and prepare a resource/phone list.
- Review and modify existing maintenance contracts, or negotiate new contracts as necessary.
- Train users how to use the back-up procedures outlined in the contingency plan.
- Determine triggers that will initiate a work-around, or activation of contingency plan.
- Test AIS contingency plans to uncover any missing actions. Tests may need to include contractors and vendors. Critique the test, correct problems; and, if possible, test again.

Development of an AIS Year 2000 contingency plan

The AIS Team, working in concert with the BCPW, should coordinate the following activities so that the VA health care facility is properly prepared and potential disruptions related to the Year 2000 are minimized.

a. **Functional Unit Managers complete their respective templates** by mapping functions to dependent AIS systems, suppliers, or equipment. Once all the critical systems are mapped, they must be sorted in mission-critical order. The purpose of this exercise is to ensure that the AIS Team focuses its contingency planning efforts appropriately and allocates its resources to high-priority corrective actions first.

b. **Conduct a risk assessment** by determining the potential for Year 2000 date-related failures for all critical AIS systems identified in the Functional Unit Templates. Each AIS system should be assessed with respect to potential risk for a Year 2000 date-related failure and the impact of such a failure on operations. Year 2000 risks may include system failures, or malfunctions and information and service disruptions of all kind. A sample risk assessment form is provided as Supplement 2, Page 48.

   Consider ranking as “Low, Medium and High” risk based on the consequences of such events as:

   - ❑ Loss of vital records and data
   - ❑ Loss of communication systems
   - ❑ Possible failure of computer security systems
   - ❑ Inability to use critical programs
   - ❑ Extended periods of operating at less than normal efficiency
   - ❑ Power failures and fluctuations, interruptions in gas, water, and other utilities
   - ❑ File overwrites and deletions

   Efforts and resources expended for corrections can then be made proportional to the risk. The AIS Team should also consider possible external factors that would have an impact upon AIS systems; such as, a disruption in transportation systems having an effect on the availability of vendor support. These expected and possible events may or may not have an obvious relationship to the Year 2000 problem, but may be part of a scenario that the facility must deal with at the same time that it is dealing with the Year 2000 problem.

c. **Develop back-up procedures and contingency plans** to reduce or eliminate the potential effect of Year 2000 problems. Mitigation strategies may have already been developed by the facility for reasons other than Year 2000 problems. For example, a manual work-around process may have already been designed for use in the event of an unpredicted system failure, or plans to move operations to another site may have already been developed for use in the event of a major fire or natural disaster. These strategies should be reviewed for modification as part of the Year 2000 contingency plans.

Contingency actions cover four time periods:

1. Actions to be taken in advance of the potential occurrence (disaster avoidance).
2. Actions to be taken at the onset of an undesirable event to limit the level of damage, loss, or compromise of assets.
3. Actions to be taken to restore critical functions.
4. Actions to be taken to reestablish normal operations.

Once all risks are ranked (AIS systems are prioritized and the potential for Year 2000 failure determined), the AIS Team, in collaboration with the BCPW must decide which back-up procedures to put into place. One viable option is simply to accept the consequences of risk, particularly if the impact is not extreme and the probability of the risk becoming a reality is low, or the proposed back-up plan creates more risk. In addition, a feasibility study will indicate whether a strategy is only viable for a short period of time and whether the team needs to develop a transitional strategy that can be sustained for a longer time.

If a mitigation strategy requires data to be recorded in another format or service to be reduced or changed, the AIS Team should also develop a plan for restoring the data to the computer system once it has been repaired, or after service has been restored. When no existing strategy adequately addresses an identified Year 2000 risk, the AIS Team may need to create unique, alternative solutions to problems. Other resources may need to be identified and used as part of such solutions.

d. **Share contingency plans and procedures with functional unit managers and the BCPW.** The AIS Team should share its contingency plans with all involved parties, particularly the functional unit managers and the BCPW. Progress should be reported to the BCPW on a regular basis. Any decision by the AIS Team to not mitigate a particular risk, for whatever reason, should be reviewed and approved by the BCPW.

e. **Train staff and Test Contingency Plans.** A set of manual procedures should be rehearsed. At the very least, the mitigation strategies should be discussed, step-by-step, in detail with the people who will implement the procedures.

f. **Critique and Evaluate Tests.** It is very important that the AIS Team along with the BCPW take the time to evaluate contingency plan drills. This evaluation should include at least the following:

- ❑ The accuracy of the risks that were identified.
- ❑ The effectiveness of tested mitigation strategies.
- ❑ The value of back-up plans.
- ❑ Areas where additional training of staff is needed.

g. **Update and Modify contingency plans are necessary.** AIS back-up procedures should be modified based on the critique of the test and evaluation of contingency plans.

3.4.2 Execution Phase

There are a number of actions that health care facilities should take during the Execution Phase—72 hours prior and 72 hours after transition of the century—to mitigate potential disruptions in critical operations due to Year 2000 date-related problems. The Chief, IRM or CIO should coordinate these actions in concert with the health care facility's Command Center and Business Resumption Team.

Business Resumption Team—The Business Resumption Team is the group of technical experts who are prepared to respond to critical system failures. The team should consist of staff who can assess and restore failed systems. Section 2.1.4.4, Internal Operations, outlines the specific duties and membership of the Business Resumption Team. The ***V****IST****A*** systems manager, network manager, Information Security Officer, and telecommunications specialists should be included on this team.

The Business Resumption Team should handle problem calls throughout the facility and coordinate their actions including providing periodic status reports to the Command Center. The Business Resumption Team will determine the level of effort necessary to restore the system, or service and apply the requisite personnel to restore service. Members of the Business Resumption Team should be available on site during the Execution Phase, or they should be on-call through the use of home telephone, pager, or cellular telephone.

In managing AIS systems during the Execution Phase, Chiefs, IRM or CIO should:

- Ensure that the proper personnel will be in place to effect a smooth Year 2000 transition.
- Perform a backup of all systems, utilities, and application software, data files, and associated documentation for use in back-up and recovery operations.
- Consider shutting down selected critical AIS systems just prior to the Year 2000. After the New Year, bring these systems up individually and put them back on line.
- If there is a ***V****IST****A*** failure, VHA and vendor personnel jointly assess and determine the severity of the situation.

3.4.3 Post-Execution Phase

Seventy-two hours after transition to the century, health care facilities should assess all AIS systems to determine if they are functioning appropriately.

- After a return to normal operation at the facility, correct those AIS problems that were not addressed during the Year 2000 crisis.
- Prepare an after-action report of the Year 2000 experience and apply what is learned to current AIS contingency plans.

A boilerplate AIS Year 2000 Contingency Plan policy is provided as Supplement 3, page 49. This sample policy should be customized for each individual health care facility.

Supplement 1

Potential AIS Systems Failures or Operational Problems Due to Year 2000

Computer System Applications Risks

Data Input Problems, e.g.

- data cannot be received
- data received is non-compliant
- batch processing scheduling system fails

Application Failure, e.g.

- application aborts
- application malfunctions
- date is wrong, but data is correct
- data is incorrect and immediately detectable
- data is incorrect and not immediately detectable

Output Data Transmission Problems, e.g.

- (correct) data cannot be transmitted to target in the usual manner
- incorrect data is transmitted

Hardware Failure, e.g.

- system fails
- security system fails and allows anyone in
- security system fails and allows no-one in

Back-up/Archiving Failure, e.g.

- back-up system fails
- archiving system erases files in error

Business Process Control Systems Risks

Input Data Problems, e.g.

- data cannot be received
- data received is non-compliant
- batch processing scheduling system fails

Goods and Services Supply Interruptions, e.g.

- supplier cannot deliver essential goods
- system maintenance staff not available (too busy fixing other’s systems)

Embedded System Failure, e.g.

- equipment stops functioning
- equipment malfunctions
- date is incorrect, but data is correct
- data is incorrect and immediately detectable
- data is incorrect and not immediately detectable

Data Storage Hardware and Software Failure, e.g.

- hardware failure
- incorrect data storage

Output Failure, e.g.

- (correct) data cannot be transmitted to target in the usual manner
- incorrect data is transmitted

Physical Facility Risks

Infrastructure Service Supply Interruption, e.g.

- electrical power failure
- gas line shut down
- water supply failure
- water treatment plant failure
- telecommunication lines are down
- elevators shut down

Security System Breakdown, e.g.

- entrance control security system lets anyone in
- entrance control security system does not allow anyone in
- fire alarm fails
- vaults will not open/lock

Telecommunications Equipment Failure, e.g.

- telephone switch fails
- fax machine fails
- email service fails
- telecommunication transmission lines are down

Supplement 2

Risk Assessment Form

AIS SYSTEM: ____

CONTACT OR SUPPORT SPECIALIST: ______________________________

Section 1. Criticality of the AIS System (Check one)

_____ **High**: The facility could not accomplish its mission without the system.

_____ **Medium**: The system is necessary for the facility to perform its mission in a cost-effective and timely manner.

_____ **Low**: The system improves productivity or saves costs but is not essential to operations.

Section 2. Risk of Interruption Due to a Year 2000-related Problem (Check one)

_____ **High**: The system uses date sensitive program/chips, and the vendor has given no assurance that the device is compliant.

_____ **Medium**: The vendor has stated that their intent is to make all of their devices "Y2K Compliant."

_____ **Low**: The vendor has responded in writing that their system is compliant. Additionally, the health care facility has validated (tested) the device and found it to be Y2K compliant.

Section 3. Prioritizing the AIS System

Based on the assessment conducted in sections 1 and 2, the Chief, IRM or CIO should assign a priority to the AIS system to be used when allocating resources during the Pre-Year 2000 Preparation Phase and when assigning staffing during the Execution Phase.

Section 4. Back-up Procedures

What procedures are in place within the unit to capture and manually process the data that is currently run on the system? Explain:

____

____

____

Are other systems dependent on this device/application?

YES NO If yes, list the systems:

____

____

____

Supplement 3

Department of Veterans Affairs
Health Care Facility

AIS Year 2000 Contingency Plan

1. **Purpose:**

To establish and implement contingency plans intended to mitigate any potential disruption to facility Automated Information Systems (AIS) due to Year 2000 date-related problems. Such a disruption is defined as any unexpected system failure that hampers patient care, impacts on the operation, the facility, or interferes with electronic information access.

2. Policy:

Contingency Plans should be developed for all critical Automated Information Systems. The intent of such plans is to assure that users can continue to perform essential functions in the event the Automated Information Systems fail.

3. Responsibilities:

a. **The Facility Chief, IRM or CIO**

The Chief, IRM or CIO has a key role in coordinating all AIS Year 2000 contingency planning efforts. Responsibilities include:

- Incorporating AIS contingency procedures into the health care facility’s overall Year 2000 contingency plan.
- Designate an AIS Year 2000 Contingency Planning Team composed of technical experts, such as the systems manager, information security officer, supervisor of telecommunications, and network manager to work with the health care facility’s Business Continuity Project Workgroup (BCPW) or Emergency Preparedness Committee to ensure communications and plan integration.

b. **AIS Year 2000 Contingency Planning Team:**

- Review all hardware and software for Year 2000 compliance and correct any deficiencies.
- Review the AIS portion of the functional unit templates for potential Year 2000-related failures and the need for back-up plans/systems.
- Prepare a priority list of systems, servers and desktop hardware and identify those that are “mission critical.” Priorities will be based on equipment that has been identified as “mission critical” (i.e., patient care areas, laboratory and central servers).
- Identify back-up equipment and software for critical systems to be held in reserve as replacements if failures occur. This extends to vendors and back-up media needed to backup systems.

- Ensure that “mission-critical” systems such as servers, hubs, telephone closets, telephone switches, and key clinical workstations are on emergency power.
- Prepare for adequate coverage and appropriate IRM staff to cover during the Execution Phase. Prepare a “triage” plan for IRM to respond to various scenarios.
- Prepare a phone list including number of pagers and portable phones of key staff for use by Business Resumption Team and the Command Center. Identify necessary vendor support and prepare a resource/phone list.
- Review and modify existing maintenance contracts, or negotiate new contracts as necessary.
- Teach users how to use alternate AIS resources identified in the contingency plan.
- Determine triggers that will initiate a work-around, or activation of contingency plan.
- Test AIS contingency plans to uncover any missing actions. Schedule the test with the support of contractors and vendors. Critique the test, correct problems and, if possible, test again.

c. **Functional Unit Managers are responsible for:**

- Identifying all critical applications processed on facility automated information systems, including desktop systems.
- Ensuring that all critical automated information stored on desktop systems is adequately backed up and stored in a secure location.
- Developing and maintaining the unit’s Functional Unit Template, which outlines the procedures for protection and recovery of physical files, as well as manual procedures to be used in the event that AIS systems are out of service.
- Communicating contingency plans to all users within the functional unit. Individual responsibility and authority must be clearly defined and communicated. Coordinating the activation of the Unit’s contingency plan during an emergency.

4**. Procedures:**

The AIS Team working in concert with the BCPW should coordinate the following activities to ensure that the health care facility’s contingency plan contains all of the elements necessary to minimize threats and to recover from disruptions to AIS operations.

a. **Functional Unit Managers will complete their respective templates** by mapping functions to dependent AIS systems, suppliers, or equipment (determining the applications and equipment that are most vital to the operation of the health care facility).

b. **Assess the risk of AIS system failure due to a Year 2000 date-related problem.** The AIS Team in concert with the BCPW should determine which AIS systems are most vital to operations and assess the likelihood of AIS system failure. The risk assessment tool provided in Supplement 2, page 45 may assist with this activity.

c. **Based on the data gathered in a. and b, develop contingency plans and a schedule for implementation.** Once all risks are ranked (critical AIS systems are prioritized and the potential for Year 2000 failure determined), the AIS Team, in collaboration with the BCPW must decide which back-up procedures to put into place. Mitigation strategies may have already been developed by the facility for reasons other than Year 2000 problems. Determine the value of each critical AIS system that is at risk and compared with the cost of the proposed back-up plan.

d. **Share contingency plans and procedures** with all involved parties including the BCPW and the functional unit managers.

e. **Train staff** on back-up procedures and alternative manual operations.

f. **Test plans and modify as needed** to reflect changes in staffing levels, computer and network back-up procedures and use of manual procedures. The AIS Team should be included in facilitywide and VISN-wide Year 2000 drills.

g. **Critique and Evaluate tests.**

h. **Update and modify contingency plans as necessary.**

5. References

OMB Circular A-130, Management of Federal Information Resources
VA Manual MP-6, Automated Data Processing
M-11 (DRAFT)
FIPS Publication 87, Guide for AIS Contingency Planning

6. Recission

7. Expiration Date

8. Follow-up Responsibility